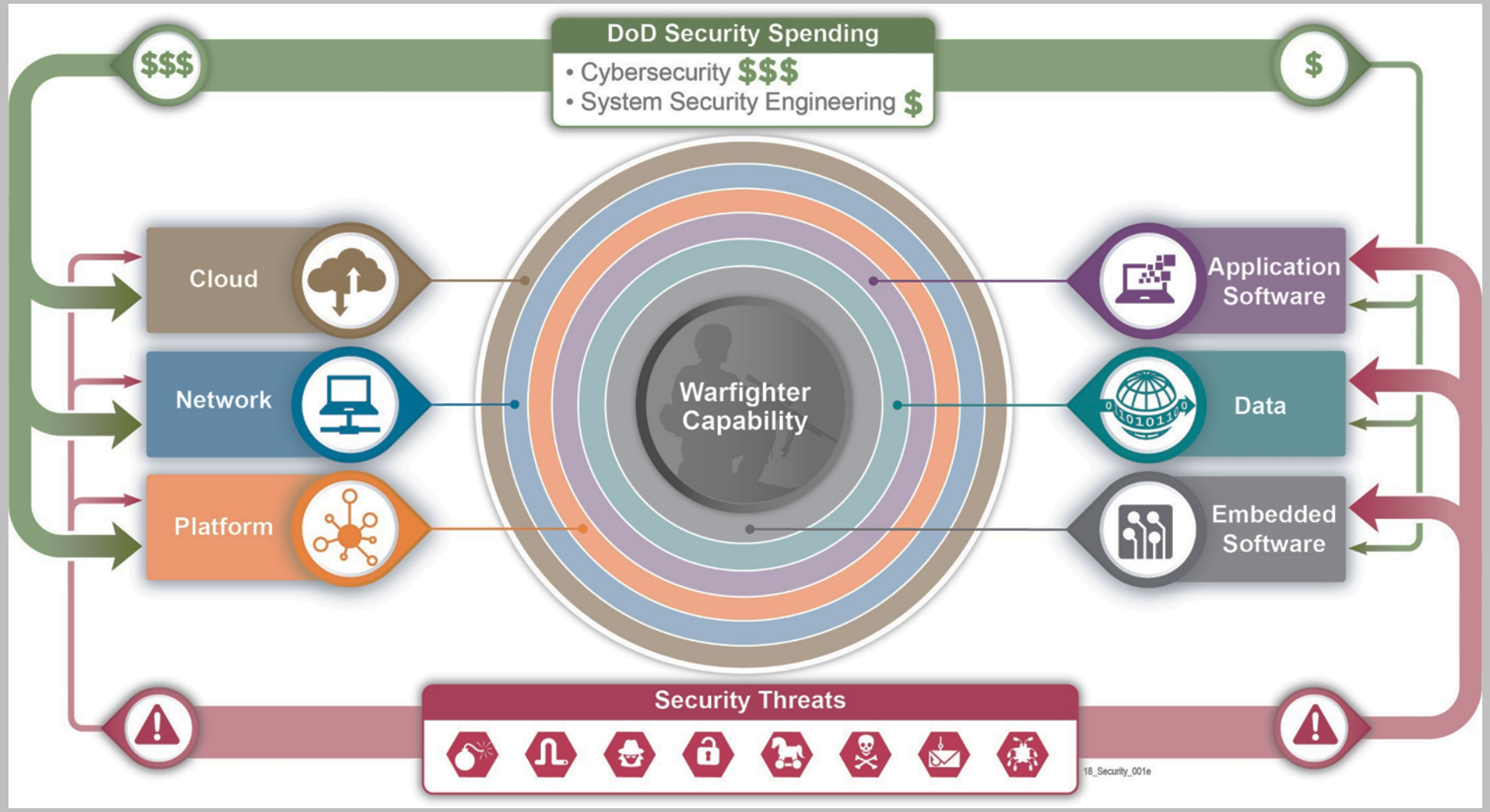
Engineering and Assurance for the Life Cycle Logistician

Mr. Thomas Hurt
Director, Joint Federated Assurance Center (JFAC)
OUSD(R&E)

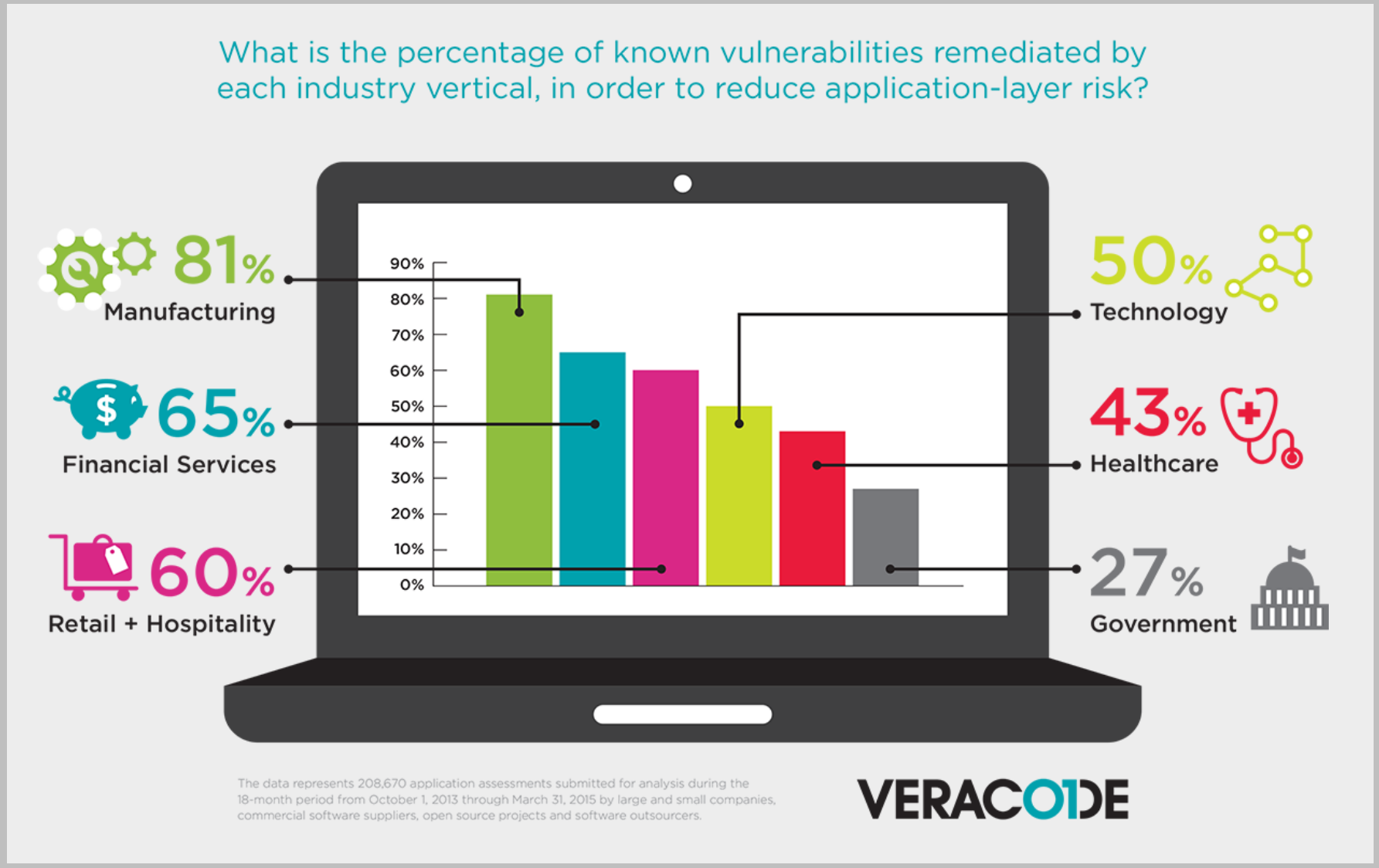
2019 Product Support Manager (PSM) Workshop
Joint Base Andrews, MD | May 15, 2019

Department of Defense Security Spending



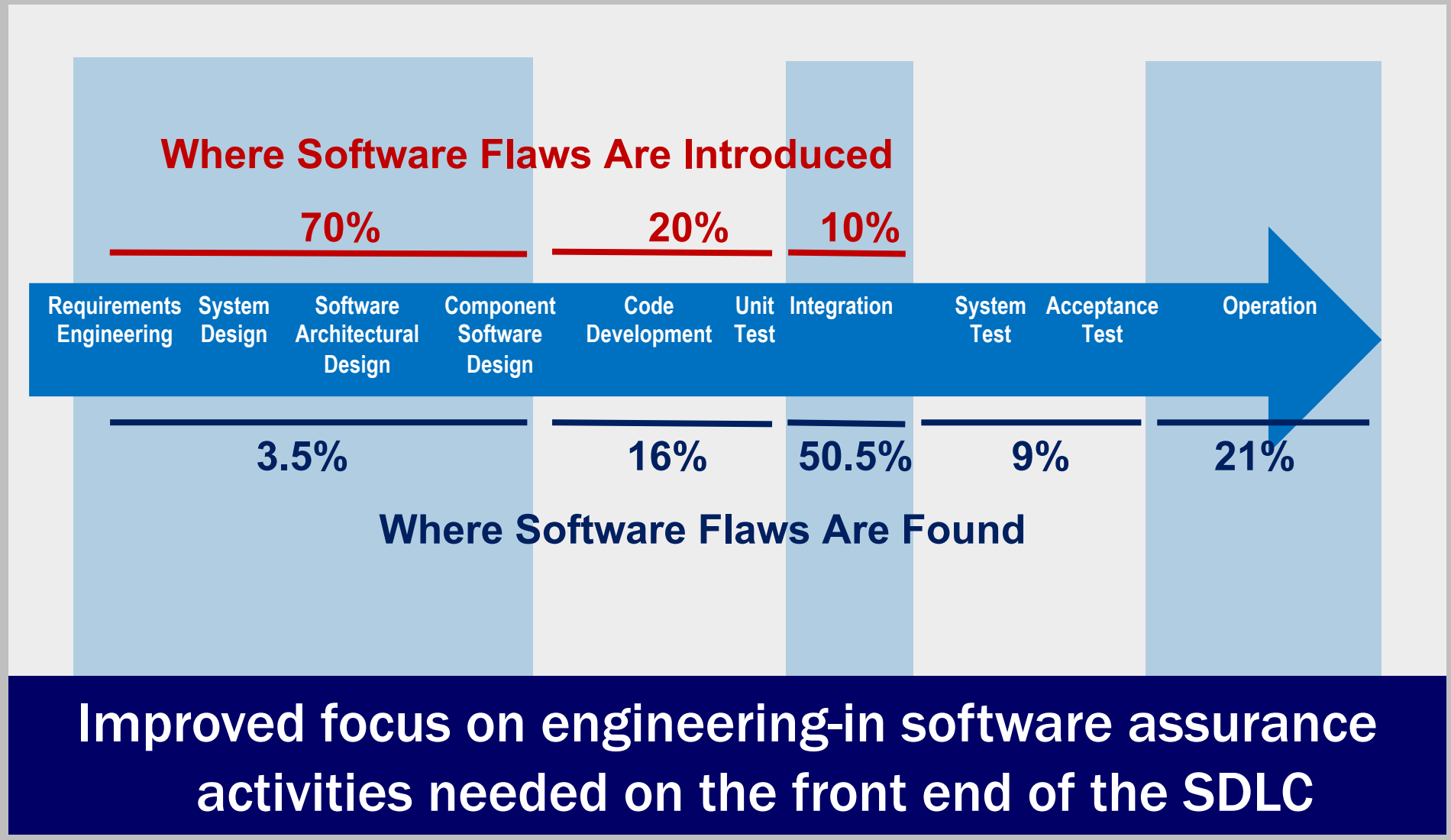
84% of breaches exploit the vulnerabilities in the application, yet funding for IT defense vs. software assurance is 23 to 1.

Who Fixes the Most Vulnerabilities?



Source: Veracode, used with permission: https://www.veracode.com/blog/2015/07/what-state-software-security-2015.

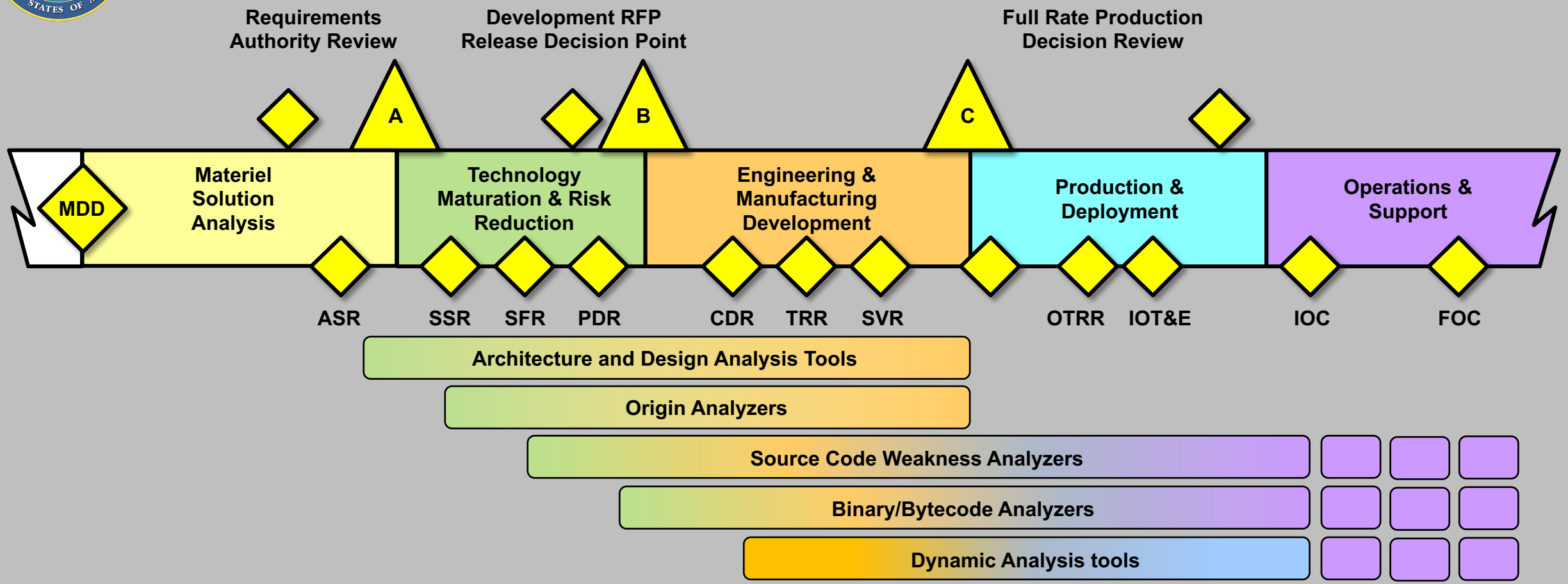
Contest: Need for Engineering-in Software Assurance Activities over the Software Development Life Cycle (SDLC)



Improved focus on engineering-in software assurance activities needed on the front end of the SDLC

Source: Carnegie Mellon University, Software Engineering Institute *(Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies), used with permission.

Tools Throughout the System Life Cycle
(Especially Sustainment)



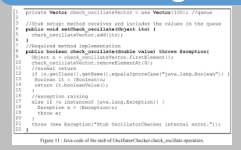
With the integration and automation of software assurance tools throughout the system life cycle, programs can make informed decisions on the identification and mitigation of risk.

Sound Systems Engineering

System Concept

Engine Control SW

Engine Monitoring SW



Control Panel

MIL-STD- 1553

Bus Controller

New System Tactical Use Threads

How will a component actually be used?

Engine Control SW (ECS) provides needed metrics

Input: Engine performance data; Output: Needed alerts/response

Read/write capabilities to data bus do needed functions

Mission Threads

What will my system do?

Engine functionality will be controlled by ECS

Engine Monitoring System will monitor engine performance

Performance issues will be transmitted by data bus to control panel

System Requirements

What is required to make my mission successful?

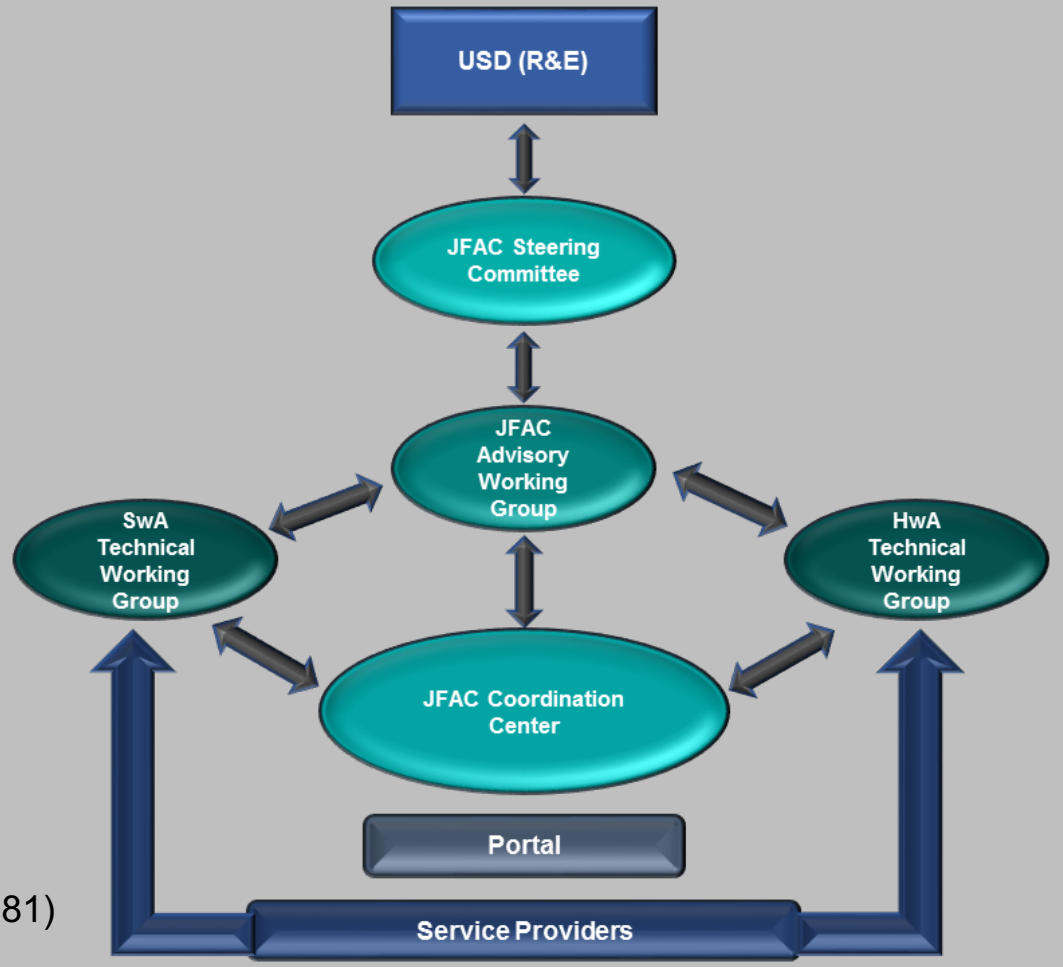
ECS has no known vulnerabilities

Monitoring SW cannot be exploited to access ESC or data bus

Secure Design/Architecture considerations for Data bus communication

JFAC Program Support Activities

- **Processes**
  - Ticket and Response Coordination
  - Software Assurance License Procurement and Distribution
  - FOC Planning and Execution
- **Working Groups**
  - Action Officer Working Group
  - Software Assurance Technical Working Group
    - SwA Portal content sub-group
  - Hardware Assurance Technical Working Group
    - Standards and best practice, field-programmable gate array (FPGA), supply chain risk management (SCRM), Technical Assessment, ASSESS and EDA assurance sub-groups
- **Applications**
  - JFAC Portal
  - Assurance Knowledge Base (AKB)
  - Cyber Integrator
- **Products**
  - Defense Acquisition University Software Assurance Course (CLE 081)
  - Security Classification Guide
  - SwA Contract Language Guidance
  - State-of-the-Art Resource (SOAR) for Software Vulnerability Detection



JFAC Operational Structure

JFAC Assurance Knowledge Base Support for Sound Systems Engineering

Development Artifacts

- Assurance assessments
- SwA tool findings
- Vulnerability prioritization (consequence and likelihood)
- Deployed assurance countermeasure rationale
- Mitigations
- Regression test results

Transition to Sustainment

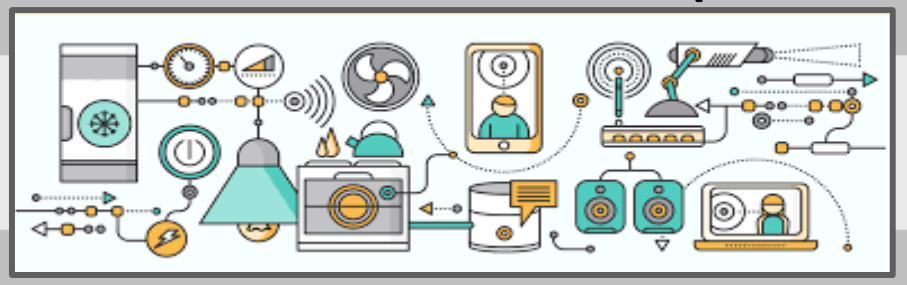
- Latent vulnerabilities and characteristics
- Mitigated vulnerabilities
- Decisions and rationale
- Vulnerability test results
- Bill of materials (BoM)
- Chain of custody

Metadata collected through the identification of tactical threads, mission threads, and systems requirements throughout development is critical to sustainment of software.

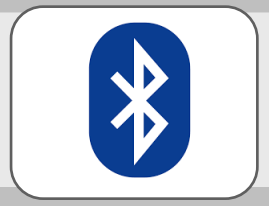
Is the Future Sustainable?

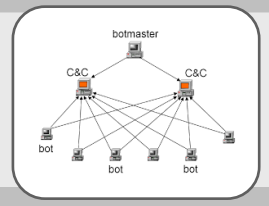
New Features/Components Added continuously

Everything is interconnected or networked (Internet of Things (IoT)



Technology continues to advance (methods of attack)





The addition of new components, changes to the network, and advancement of adversary technology creates a continuous cycle of redesign and patching to protect against unwanted access.

Last Thoughts

- Latent software vulnerabilities identified or exploited in sustainment are exponentially more expensive to fix.
- Acquisition of source code and documentation in the data rights package are expensive and ineffective steps for legacy DoD programs. Logistical data needs must be included in the development Request for Proposals (RFP).
- Sound systems engineering, implementation of SwA countermeasures, and transition of assurance rational into sustainment is critical to the protection of our weapons systems.
- JFAC needs your advocacy for development programs to use the AKB to store and retain assessment data collected throughout development, test, and deployment for use in sustainment.
- Select JFAC assessment data retention uses:
  - Vulnerability and mitigation rationale retention throughout the life cycle
  - Data mining (tracking, trending, intel, etc.)
  - Chain of custody
  - Bill of materials

https://jfac.navy.mil

DoD Research and Engineering Enterprise

Solving Problems Today – Designing Solutions for Tomorrow

DoD Research and Engineering Enterprise
https://www.CTO.mil

Defense Innovation Marketplace
https://defenseinnovationmarketplace.dtic.mil

Twitter
@DoDCTO

For Additional Information

Mr. Tom Hurt

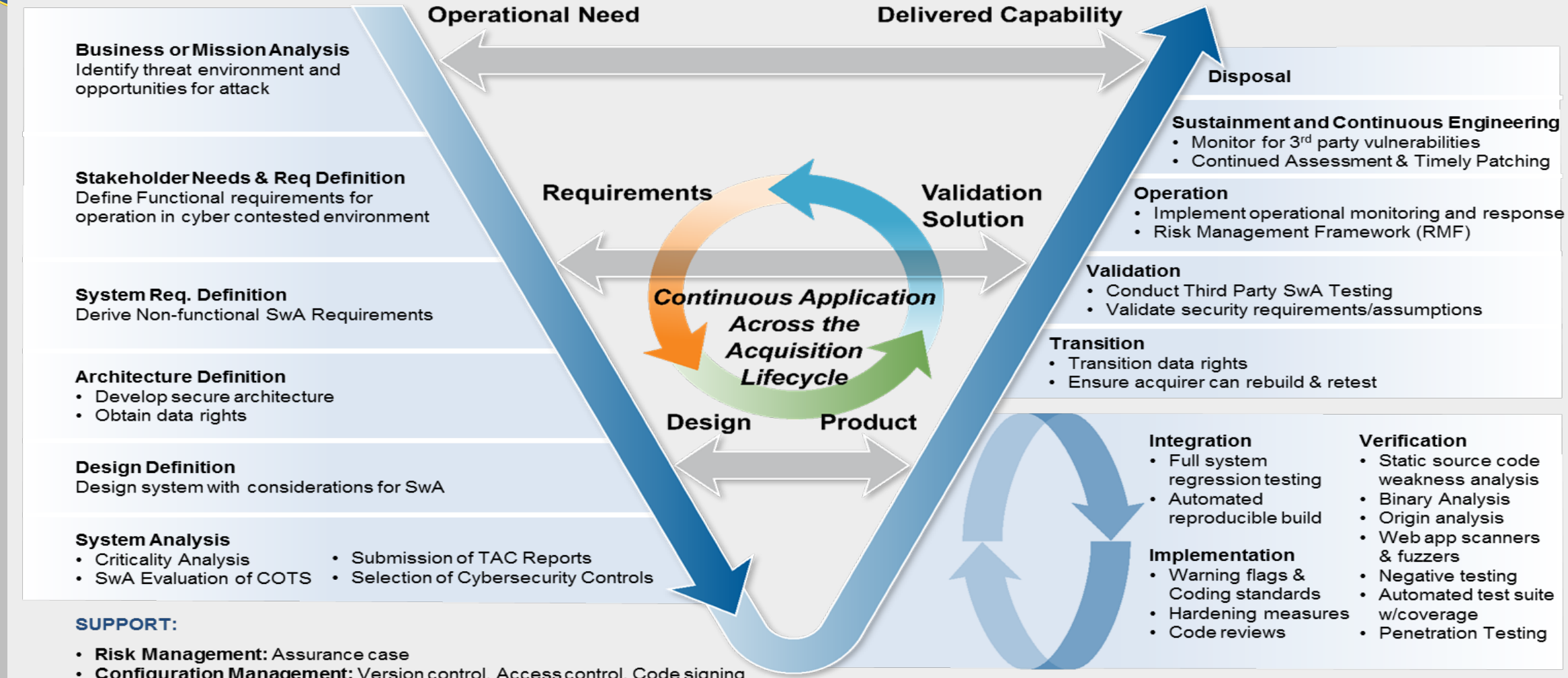
Director, JFAC / Deputy Director, Software Assurance
Strategic Technology Protection and Exploitation

Office of the Under Secretary of Defense
for Research and Engineering

571-372-6129

thomas.d.hurt.civ@mail.mil

Engineering Software Assurance into the Life Cycle



SUPPORT:

- **Risk Management:** Assurance case
- **Configuration Management:** Version control, Access control, Code signing
- **Measures & Metrics**

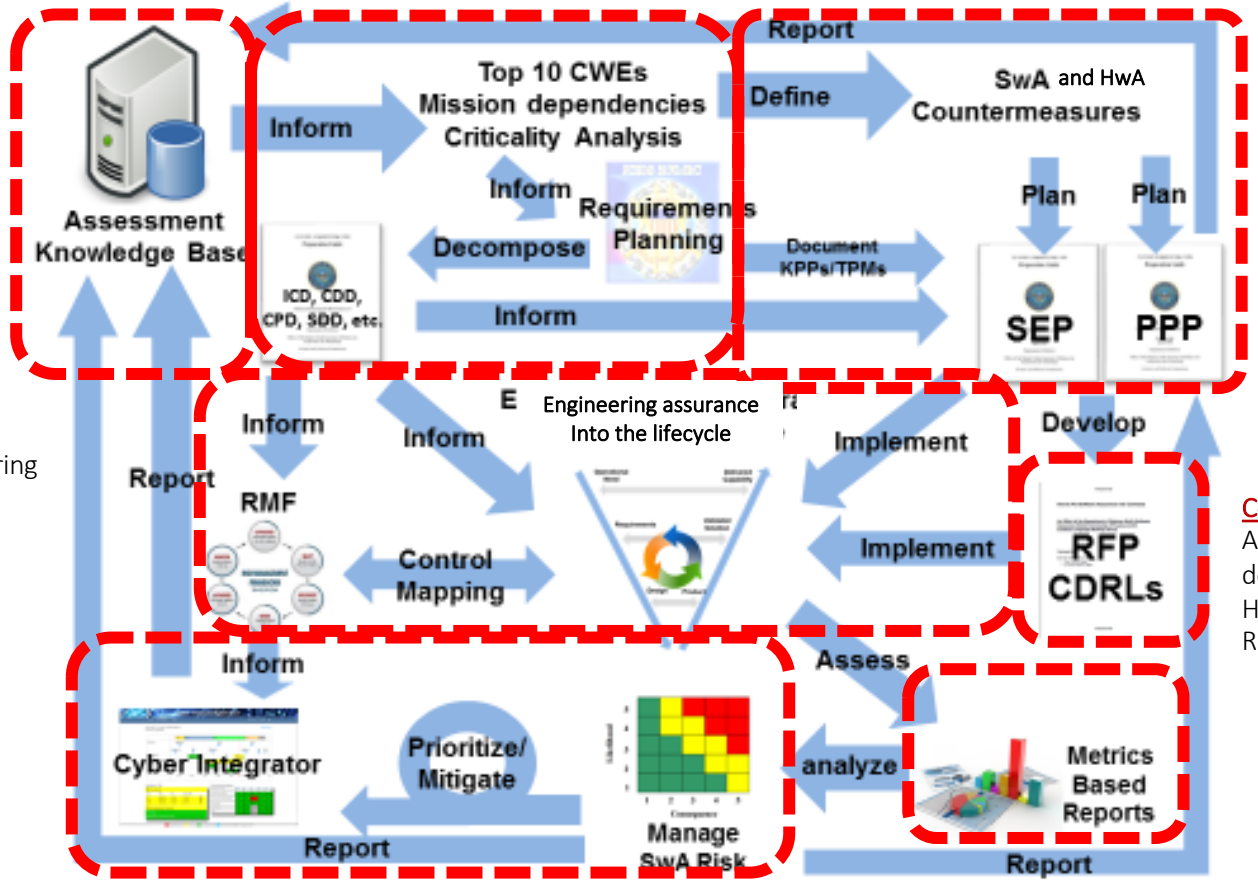
NOTE: *Lifecycle processes typically occur simultaneously, **not** in sequence; see ISO/IEC 15288 & 12207*

NOTE: *Implementation, Integration & Verification are often performed continuously & simultaneously with the aid of IDEs & other tools.*

JFAC Service Provider Capabilities

Software and Hardware Assurance (SwA and HwA) Requirements Support:
Identification of applicable SwA and HwA requirements from policy, standards, instructions, and guidance

Knowledge Source:
Identification of applicable SwA and HwA assessments and attack information from the AKB



Program Protection Plan (PPP) & SSE Planning:
Assistance with PPP development and the planning of SSE activities and countermeasures, to include SwA and HwA

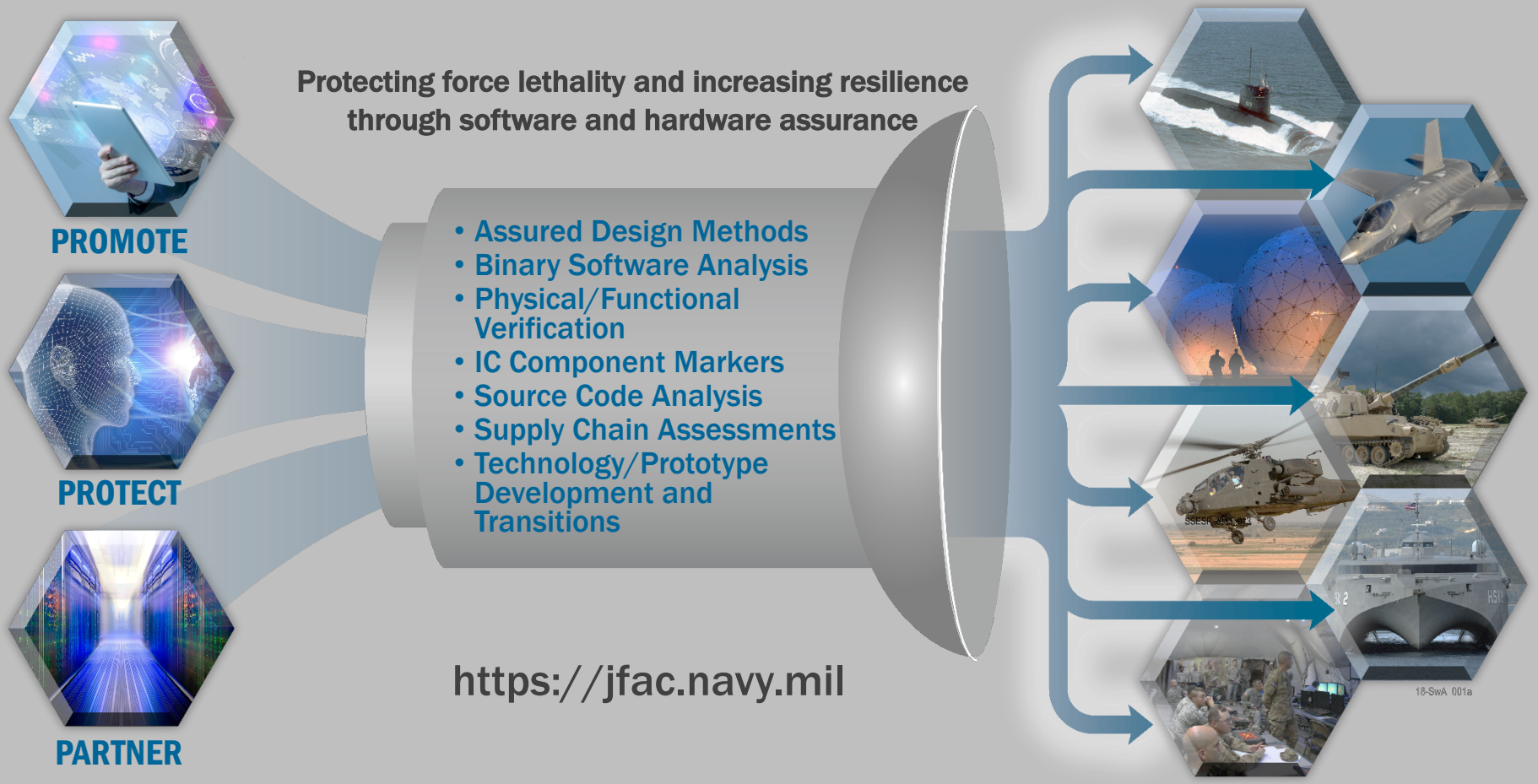
Subject Matter Experts (SMEs):
System security engineering (SSE) support during lifecycle, e.g., secure architecture & design, criticality analysis techniques, supply chain assurance (SCRM), SETR criteria, sustainment support, etc.

Contract Assistance:
Assist programs with the development of SwA and HwA contract language for RFPs and CDRLs

Third Party Assessment: Assistance in program evaluation and risk assessments, including bitstream analysis, hardware functional verification, static source code analysis, dynamic binary analysis, static binary analysis, web application analysis, database analysis, and mobile application analysis

Metrics Assistance:
Assist programs with the identification, benchmarking, and collection of SwA and HwA related metrics (contract, progress, TPMs, …)

Joint Federated Assurance Center (JFAC) Capabilities



- Federated laboratory capability of expertise and tools for vulnerability detection and analysis
- Support program offices with software and hardware assurance expertise and capabilities
- Stakeholders - Army, Navy, Air Force, National Security Agency (NSA), Defense MicroElectronics Activity (DMEA), OUSD(R&E), DoD CIO, Defense Information Systems Agency (DISA), National Reconnaissance Office (NRO), Missile Defense Agency (MDA), OUSD(A&S)